ISRG and Privacy
Preserving Measurement

Tim Geoghegan
Internet Security Research Group
timg@letsencrypt.org
IETF 112, November 10 2021
Conventional telemetry is a privacy risk

- Conventional telemetry is a liability for data collectors
  - Increasing regulatory requirements (GDPR, CCPA) are expensive to implement
  - Stored telemetry is a very attractive target for attackers
- Novel cryptographic techniques like Prio and Heavy Hitters make it possible to do better, but--
  - There's nothing out there to solve this problem for small organizations and it's very easy to get wrong
  - Even for organizations that employ cryptographers and security teams, MPC protocols for private measurement require external trusted partner
- ISRG wants to build services that make private measurements easy, for everyone, just as Let's Encrypt did for TLS
ISRG's private measurements public utility

● **PPM/PRIV aggregator-as-a-service**
  ○ Data collectors may run their own aggregator with ISRG's, or choose two from a public pool of available aggregators

● **Open source aggregator server**
  ○ Container images or binaries, easy to deploy into a data collector's existing server infrastructure

● **Open source client libraries**
  ○ Client libraries provided in languages chosen to facilitate adoption (e.g., Swift for iOS, Javascript for the web, Kotlin for Android)

● **An open standard is crucial to interoperability, all the more in an MPC setting**
Case study: Exposure Notifications Private Analytics

- Private measurements tradeoffs
  - More servers -> greater risk of failure
  - Compute and network overhead
  - Can't make arbitrary post-hoc queries
- Apple, Google, ISRG, Linux Foundation Public Health, MITRE Corporation, National Cancer Institute
- 13 U.S. states and the District of Columbia
- 2.1 million measurements/hour